Department of Homeland Security Daily Open Source Infrastructure Report for 29 June 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Finextra reports a worker at HSBC's Indian call center has been arrested on suspicion of selling confidential bank account details of customers to scammers, raising new fears about the security of customer data at offshore centers. (See item 5)
- The Associated Press reports police shot and wounded a man at McCarran International Airport in Las Vegas after he grabbed a three−year−old boy at knifepoint and sprinted through a security checkpoint. (See item 12)
- The Associated Press reports more than 2,200 people were evacuated from their homes near Lake Needwood in Rockville, Maryland, when water levels approached 25 feet above normal and engineers became concerned about the structural integrity of the dam. (See item 30)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *June 28, U.S. Department of Energy* — **DOE announces loans of oil from the Strategic Petroleum Reserve.** U. S. Department of Energy (DOE) Secretary Samuel W. Bodman announced Wednesday, June 28, that DOE has approved two loan requests totaling 750,000 barrels of crude oil from the Strategic Petroleum Reserve (SPR) to two Louisiana refineries.

The refineries were not receiving scheduled shipments of crude oil because of the closure of the Calcasieu Ship Channel. “The Strategic Petroleum Reserve is a national asset that can be used in times of supply disruption. This loan will allow these two refineries to continue operations and help us maintain our nation’s supply of gasoline leading into the holiday weekend,” Secretary Bodman said. ConocoPhillips' Westlake refinery will receive 500,000 barrels of West Hackberry sour crude oil and Citgo's Lake Charles Refinery will receive 250,000 barrels of West Hackberry sour crude.
Source: http://www.energy.gov/news/3789.htm

2. *June 27, Nigeria First (Africa)* — **Nigeria: Obasanjo establishes Committee On Vandalization of Petroleum Products Pipelines.** Nigerian President Olusegun Obasanjo Monday, June 26, set up a committee to assess the magnitude of the incidence of petroleum products pipeline vandalization throughout the country. The President tasked the committee to also identify the immediate and remote causes of the vandalization and those involved, and recommend measures of eliminating the harmful incidence. Vandalization of petroleum products pipelines which usually occurred in the night, was more prevalent in Lagos, Warri, Port Harcourt, and Enugu areas while it had also become noticeable in the northern states.
Source: http://allafrica.com/stories/200606270066.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *June 28, ABC 7 Chicago* — **Crews clean up diesel spill on expressway.** Chicago firefighters cleaned up a diesel spill of nearly 100 gallons on the Bishop Ford Freeway Wednesday morning, June 28. Several lanes were shut down as a result.
Source: http://abclocal.go.com/wls/story?section=local&id=4313391

4. *June 27, Associated Press* — **Carbon monoxide leak at Maryland hotel kills two.** Two people died and two were hospitalized Tuesday, June 27, in Ocean City, MD, because of a carbon monoxide leak at the Days Inn Oceanfront hotel. The leak was reported just before 2 p.m. EDT and parts of the hotel were evacuated as a result.
Source: http://www.thevictoriaadvocate.com/24hour/nation/story/33191 99p−12226249c.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *June 28, Finextra* — **Indian call center worker arrested for HSBC fraud.** A worker at HSBC's Bangalore call center has been arrested on suspicion of selling the confidential bank

account details of UK customers to scammers. Data worker Nadeem Kashmiri, 24, has been charged with hacking into computers and breaching confidentiality agreements and privacy laws. According to press reports hundreds of thousands of dollars were stolen from the accounts of 16 UK customers after Kashmiri allegedly sold bank details to scammers while working at the call center. The fraud was detected by internal systems at the call center. A spokesperson for HSBC told reporters that all affected customers had been notified and refunded and the bank intends to "pursue a conviction as aggressively as possible." The incident raises new fears about the security of customer data at offshore centers and follows a number of high−profile breaches last year.
Source: http://finextra.com/fullstory.asp?id=15506

6. *June 28, Websense Security Labs* — **Phishing Alert: The Municipal Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of The Municipal Credit Union, which is based in New York. Users receive a spoofed e−mail message, which claims that their account has been locked due to excessive number of login attempts. The message provides a link to a phishing Website that requests users to log on and provide account details.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =539

7. *June 28, Federal Times* — **Thrift Savings Plan to stop using Social Security numbers.** In a few months, the 3.6 million participants in the Thrift Savings Plan (TSP) will begin using account numbers instead of Social Security numbers to access their retirement accounts. TSP administrators are switching to randomly generated account numbers to enhance security and protect participants' Social Security numbers from being stolen, said Mark Hagerty of the Federal Retirement Thrift Investment Board, which oversees the TSP. Converting everyone to account numbers instead of Social Security numbers is rather simple to do technically, Hagerty said. A more challenging task will be educating plan participants on the change before it's put in place. TSP has masked Social Security numbers when a participant enters them online. TSP includes only the last four digits of the Social Security number on statements mailed to participants. The plan is considering other security enhancements, including being able to trace laptops that are lost or stolen and remotely erase any personal information contained on them, Hagerty said.
Source: http://federaltimes.com/index.php?S=1891951

8. *June 27, Associated Press* — **Experts to form ID theft research center.** An alliance of businesses, colleges, and federal crime fighters will combine their expertise at a new research center that will study the problems of identity theft and fraud. Founding partners of the Center for Identity Management and Information Protection include LexisNexis Inc. and IBM Corp., the U.S. Secret Service, and the FBI. The center will be established in New York at Utica College. Research will focus on critical issues in identity management, information sharing policy, and data protection, said Dr. Gary Gordon, a Utica College professor and expert in cybercrime and identity fraud. One of the initial research projects at the center will examine current and emerging criminal groups that perpetrate identity fraud and theft, with a focus on their methods of operation. It also will look at developing stronger identity authentication systems. The center will share its research through training sessions, symposiums, publications, and its Website.
Center for Identity Management and Information Protection: http://www.cimip.org

Source: http://news.yahoo.com/s/ap/20060627/ap_on_hi_te/identity_theft_center;_ylt=AmN_JkA3ygx7hmeu_XZgi9QjtBAF;_ylu=X3oDMTA2Z2szazkxBHNlYwN0bQ

9. *June 23, BusinessWeek* — **ID theft: More hype than harm.** All told, as many as 88 million Americans −− more than one in four −− had digital data exposed in the past 18 months. With each report, the feeling of helplessness grows. But for all of the drama over ID theft, what is not often pointed out is how rarely it results in actual financial loss for consumers. There's reason to believe that the actual losses may be a little more than a tenth of the $48 billion annual estimate that often gets thrown around. In fact, at the same time that regular folks are getting the wits scared out of them about security breaches, experts in the field are growing less worried about the impact. Law enforcement officials, who braced for a wave of financial fraud following all those well−publicized incidents, admit they've been struck by the lack of follow−through by criminals. "What we've seen has not been significant...Given the high profile, we would have expected to have seen more," says Daniel Larkin, who heads the Internet Crime Complaint Center for the FBI.
Source: http://biz.yahoo.com/bizwk/060623/b3991041.html?.v=1

[Return to top]

Transportation and Border Security Sector

10. *June 28, Department of Transportation* — **Federal freight locomotive crashworthiness standards to improve protection for train crews.** Train crews involved in a locomotive collision will have a better chance of survival with reduced injuries as a result of the first−ever federal freight locomotive crashworthiness standards issued on Wednesday, June 28, according to Federal Railroad Administrator Joseph H. Boardman. The regulation is intended to prevent the locomotive cab from being crushed during a head−on collision with another locomotive, or when it strikes the rear of another train, a shifted load on a train on an adjacent track, or a vehicle at a highway−rail grade crossing, Boardman said. The crashworthiness standards include upgraded structural elements such as stronger collision posts and the addition of anti−climbing equipment to keep the locomotive upright and in−line on the tracks after a collision occurs, Boardman said. The interior of the locomotive cabs also will need to be reconfigured to soften many sharp edges and provide better emergency lighting and exits. In addition, fuel tanks will be strengthened to prevent spills that could lead to a fire, he added. The rule changes will be required for locomotives newly manufactured or rebuilt beginning in January 2009.
Final rule: http://www.fra.dot.gov
Source: http://www.dot.gov/affairs/fra0706.htm

11. *June 28, Transportation Security Administration* — **Canine graduates bolster ability to detect explosives at airports, mass transit systems.** The Transportation Security Administration (TSA) announced on Wednesday, June 28, the graduation of 24 members of its National Explosives Detection Canine Team Program. The teams are assigned to mass transit systems in Washington, DC (Washington Metropolitan Area Transit Authority); Chicago (Chicago Transit Authority) and San Diego (San Diego Trolley, Inc.); and airports in Atlanta, Boston, Chicago, Denver, Los Angeles, Phoenix, Dayton, OH, Ft. Myers, FL, Buffalo, NY,

Washington DC, Norfolk, VA, Seattle, San Francisco, and Oakland, CA. During training, officers were provided instruction on handler skills and explosives safety along with the safe handling and accountability of explosives canine training aids. Teams spent much of their time searching for explosives in specialized indoor and outdoor training labs that included an aircraft fuselage, a terminal area and a cargo warehouse. The teams also practiced searching luggage and a parking lot filled with vehicles. Because canine teams combine excellent mobility with reliable detection rates, their use has evolved to include searching areas in response to bomb threats at airports and mass transit terminals, and aircraft, trains, luggage, cargo, and vehicles, as well as serving as a proven deterrent to would−be terrorists.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 01fc784

12. *June 28, Associated Press* — **Police shoot man at Las Vegas airport.** Police shot and wounded a man at McCarran International Airport in Las Vegas on Tuesday, June 27, after he grabbed a three−year−old boy at knifepoint and sprinted through a security checkpoint, authorities said. The 25−year−old man snatched the boy at a toy store in an unsecured area just outside a gate area at McCarran, officials said. The child was not harmed and was returned to his mother. The man ran about 20 yards, making it through an exit lane before being confronted by three officers. One officer used a Taser gun to stun the man, police said. He dropped the child, then charged at the officers, said police spokesperson Jose Montoya. Two officers fired once each. Elaine Sanchez, airport spokesperson said, "As soon as the breach occurred, the police were in place, and the system worked."
Source: http://www.boston.com/news/nation/articles/2006/06/28/police_shoot_man_at_las_vegas_airport/

13. *June 27, Government Accountability Office* — **GAO−06−910T: Public Transportation: Preliminary Information on FTA's Implementation of SAFETEA−LU Changes (Testimony).** The Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA−LU) authorized a significant level of investment −− over $52 billion −− for federal transit programs. SAFETEA−LU also added new transit programs and made changes to existing programs, including the New Starts and Job Access and Reverse Commute (JARC) programs. The New Starts program is a discretionary grant program for public transportation capital projects. The JARC program is intended to improve the mobility of low−income individuals seeking work. SAFETEA−LU authorized $8.6 billion for these two programs. The Federal Transit Administration (FTA) manages both of these programs. This testimony discusses the Government Accountability Office's (GAO) preliminary findings on the (1) changes SAFETEA−LU made to the New Starts program, (2) changes SAFETEA−LU made to the JARC program, and (3) issues that may be important as FTA moves forward with implementing the act. To address these objectives, GAO interviewed FTA officials, sponsors of New Starts projects, and representatives from industry associations and reviewed FTA's guidance on the New Starts and JARC programs and federal statutes, among other things.
Highlights: http://www.gao.gov/highlights/d06910thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−910T

14. *June 26, Government Computer News* — **Coast Guard secures facilities with biometrics RFID system.** Since November, use of RapidGate ID cards, has helped the Washington, DC, Coast Guard campus identify three potential vendor employees who had served time for murder, one registered sex offender, two working under false names, and others with multiple

identities or who had lied about their criminal history, said Wayne Truax, Coast Guard's chief of security and safety for the headquarters support command in Washington. Also, Fort Lewis, WA, which has been using RapidGate for two years, is using biometrics to authenticate and identify vendors, and RFID to track vehicles. The RFID tag is connected to a vendor's vehicle so the Coast Guard knows when it enters or leaves the facility. About 700 vendors and 4,000 people enter Fort Lewis every day, and vendors can enter in as little as 12 seconds. In DC, about 50 vendors and 105 card holders use RapidGate, which the Coast Guard runs in parallel with its physical−access control system, called Maxxess.
Source: http://www.gcn.com/print/25_17/41095−1.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

15. *June 28, WBKO (KY)* — **Blue mold threatens tobacco crop.** Most cases of blue mold are in Eastern Kentucky but farmers are afraid it will spread farther. "Blue mold is a fungal disease of tobacco by an air born spore," said University of Kentucky plant pathologist Kenny Seebold. Blue Mold has the potential to destroy an entire tobacco crop. Specialists say most of the states blue mold problems this year originated in plants shipped from out of state.
Source: http://www.wbko.com/news/headlines/3241991.html

16. *June 28, Stop Soybean Rust News* — **Soybean rust on Georgia kudzu called new infection in old site.** New Asian soybean rust is growing on kudzu in a Brooks, GA, site where officials say all known infected plant parts were destroyed this winter. Rust is also spreading at the rate of five feet per week within the Miller, GA, kudzu site. University of Georgia plant pathologist Layla Sconyers reported: "We found soybean rust on a kudzu sample collected June, 26, 2006 from Brooks, Georgia. To date, soybean rust has not been found on soybeans in Georgia. Soybean rust was found in this particular location in February, and to our knowledge, we destroyed all infected plant parts. "This infection seems to be a 'new' infection −− perhaps spores were brought into the area by the Alberto system that came through the area a couple of weeks ago."
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=864

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

17. *June 28, WABC (NY)* — **Contaminated water in Nassau County.** Customers of a central Nassau County, NY, water district were advised Tuesday, June 27, not to drink or use tap water for cooking, brushing teeth or making ice after high levels of a fuel additive were detected during testing. The gas additive chemical MTBE was found in the water system of the West Hempstead−Hempstead Gardens Water District. Water officials say the wells that contain MTBE were taken off line and the system is being flushed. MTBE (methyl tertiary−butyl ether) is a chemical compound manufactured by the chemical reaction of methanol and isobutylene and used as a fuel additive in motor gasoline.
Source: http://abclocal.go.com/wabc/story?section=local&id=4311824

18. *June 27, Stanley News & Press (NC)* — **Chlorine leak hits treatment plant.** A chemical leak at the water treatment plant at Tuckertown Reservoir, in North Carolina, sent two employees to Stanly Regional Medical Center Monday, June 26. Assistant City Manager Michael Ferris said a small leak in the chemical handling room exposed two employees to chlorine gas at the Albemarle water treatment plant. The leak occurred when an employee was attempting to change a one–ton chlorine cylinder. When a valve began to leak, two employees were exposed and evacuated the building. At that time, all city employees were evacuated from the building and fenced in grounds of the water plant.
Source: http://www.thesnaponline.com/local/local_story_179080211.htm l

[Return to top]

Public Health Sector

19. *June 28, World Health Organization* — **World Health Organization updates guidelines for tuberculosis prevention.** The World Health Organization (WHO) has issued updated guidelines for the airline industry that will further minimize the risk of tuberculosis (TB) and other infectious diseases being passed from passenger to passenger on board aircraft. The "Tuberculosis and Air Travel" guidelines stipulate that people with infectious TB must postpone long−distance travel, while those with multi drug−resistant tuberculosis must postpone any air travel. To date, no case of active TB has been identified as a result of exposure on a commercial aircraft. The quality of the air on board commercial aircraft is high and under normal conditions cabin air is cleaner than the air in most buildings. Prolonged journeys of more than eight hours in a confined aircraft cabin may involve an increased risk of transmission, but the risk should be similar to that in other circumstances where people are together in other confined spaces. The guidelines also advise that aircraft ventilation systems should continue to operate when the aircraft is delayed on the ground and the doors are closed. If not in operation, ground delays should be kept to less than 30 minutes.
Guidelines: http://www.who.int/tb/publications/2006/who_htm_tb_2006_363. pdf
Source: http://www.who.int/tb/features_archive/aviation_guidelines/e n/index.html

20. *June 28, Agence France−Presse* — **China investigating potential human bird flu death in 2003.** China is investigating the possibility that a man died of bird flu in Beijing in 2003, two years before the country officially announced its first human case, the World Health

Organization (WHO) has said. In a letter to the New England Journal of Medicine, eight Chinese scientists said a man aged 24 died in late 2003 from the H5N1 strain of bird flu, although his death was initially blamed on Severe Acute Respiratory Syndrome. The Ministry of Health said it was carrying out its own tests to try to confirm the case. If confirmed, the death would not only bring forward by two years the first human fatality in China, but also change the timeframe for the outbreak of the disease regionally. The first human bird flu case China reported was in November 2005. It now has 19 officially reported human cases, of whom 12 have died. On a regional level, the first reported signs of bird flu came after the H5N1 virus caused poultry deaths in South Korea in late 2003. The first reported death from bird flu was confirmed in Vietnam in January 2004.
Source: http://news.yahoo.com/s/afp/20060628/hl_afp/healthfluchina_060628104947;_ylt=ApO5zun2VzRUzHJccnGg93.JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

21. *June 28, Bloomberg* — **Bird flu fatalities almost triple.** Bird flu fatalities have almost tripled this year as the virus spread across Asia, Europe and Africa, prompting calls for increased supplies of medicines to fight the virus and any pandemic it might spawn. Since January, at least 54 people have died from the H5N1 avian influenza strain in Azerbaijan, Cambodia, China, Djibouti, Egypt, Indonesia, Iraq and Turkey, according to the World Health Organization. That compares with 19 fatalities in Vietnam and Cambodia in the first six months of 2005. Human cases create opportunity for the virus to mutate into a lethal pandemic form. Pharmaceutical companies are racing to produce pandemic flu treatments amid concern over H5N1, which was found for the first time in wild birds and domestic poultry in 38 countries since February.
Source: http://www.bloomberg.com/apps/news?pid=20601087&sid=ahclIBD4_2ZpM&refer=

[Return to top]

Government Sector

22. *June 28, Department of Homeland Security – Office of the Inspector General* — **Homeland Security Information Network Could Support Information Sharing More Effectively.** A report released by the Department of Homeland Security Office of Inspector General assesses how well the Homeland Security Information Network, or HSIN, supports information sharing across federal, state, and local entities to prevent and deter terrorist activities; and, prepare for and respond to emergencies and natural or man−made disasters. It is based on interviews with employees and officials of the Office of Intelligence and Analysis and the Office of Operations Coordination, as well as other relevant agencies and organizations, direct observations, and a review of applicable documents.
Source: http://www.dhs.gov/interweb/assetlibrary/OIG_06−38_Jun06.pdf

[Return to top]

Emergency Services Sector

23.

June 28, Associated Press — **Nevada governor declares fire emergency.** Governor Kenny Guinn declared a state of emergency as state and federal crews put practically every available piece of equipment on the line to combat dozens of lightning−sparked fires that have burned 125 square miles of Nevada. More than 1,000 firefighters on Wednesday, June 28, were battling dozens of fires, from a 57,000−acre blaze burning out of control largely in uninhabited rangeland in northeast Nevada to a complex of a dozen smaller fires around Reno and Carson City that forced evacuations at the town of Mound House along the historic Pony Express Trail. The 125 square miles of land that has burned since lightning bolts started sparking fires over the weekend amounts to about 80,000 acres.
Source: http://www.boston.com/news/nation/articles/2006/06/28/nevada_governor_declares_fire_emergency/

24. *April 01, Bay Area Council (CA)* — **San Francisco Bay Area Council concludes report on water transportation for emergency evacuation.** Areas such as San Francisco, surrounded by water on three sides face unique challenges for evacuation in the event of a catastrophic event. Bridges, trains, public transit and tunnels could all be rendered unusable trapping the citizens. The Bay Area Council's Task Force on Disaster Recovery Water Transit addressed this issue and has proposed a system utilizing the area's water transit, or ferries, as a means of evacuation of the city.
Executive Summary: http://www.bayareacouncil.org/atf/cf/{2F567EB5−67C0−4CDA−9DD3−EC4A129D3322}/ExecutiveSummary−TransportationSpineForDisas terRecovery.pdf
Full report: http://www.bayareacouncil.org/atf/cf/{2F567EB5−67C0−4CDA−9DD3−EC4A129D3322}/EmergencyFerryReport−TransportationSpineForD isasterRecovery.pdf
Source: http://www.bayareacouncil.org/site/apps/s/content.asp?c=dkLRK7MMIqG&b=240390&ct=2173057

[Return to top]

Information Technology and Telecommunications Sector

25. *June 28, Security Focus* — **Microsoft HLINK.DLL link memory corruption vulnerability.** Microsoft HLINK.DLL is prone to a memory−corruption vulnerability. Analysis: Successfully exploiting this issue allows attackers to execute arbitrary machine code in the context of applications that use the affected library. This facilitates the remote compromise of affected computers. Failed exploit attempts will likely crash targeted applications.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18500/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18500/references

26. *June 28, IDG News Service* — **For spammers, a picture is better than 1,000 words.** Spam is again on the rise, led by a flood of junk images that spammers have crafted over the past few months to trick e−mail filters, according to security vendors. Called "image−based" spam, these junk images typically do not contain any text, making it harder for filters that look for known URLs or suspicious words to block them. Instead of a typed message, users will see only an embedded .gif or .jpeg image file urging them to buy pharmaceuticals or invest in penny stocks. Anti−spam vendor Cloudmark says that half of the incoming spam is now image−based on the "honeypot" systems it puts out on the Internet to lure spammers.

Source: http://www.infoworld.com/article/06/06/28/HNspammers_1.html

27. *June 28, VNUNet* — **Spammed Trojan hides in Word document.** IT security watchers have warned of a Trojan −− Kukudro−A −− that is being propagated via an infected Microsoft Word document in spammed e−mails, which promise information about Apple, HP and Sony laptop computers for sale. When opened the Word document attempts to install another Trojan horse −− Kuku−A −− onto the user's hard drive. The spam comes with a variety of subject lines including "worth to see," "prices," and "Hello."
Source: http://www.vnunet.com/vnunet/news/2159274/spammed−trojan−hid es−word

28. *June 27, Security Focus* — **Microsoft Internet Explorer OuterHTML redirection handling information disclosure vulnerability.** Microsoft Internet Explorer is prone to an information−disclosure vulnerability because it fails to properly enforce cross−domain policies.
Analysis: This issue may allow attackers to access arbitrary Websites in the context of a targeted user's browser session. This may allow attackers to perform actions in Web applications with the privileges of exploited users or to gain access to potentially sensitive information. This may aid attackers in further attacks.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18682/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18682/references

29. *June 27, CRN* — **Apple fixes vulnerabilities in OS X update.** Apple Tuesday, June 27, released Mac OS X version 10.4.7, which fixes several security vulnerabilities that at least one security vendor rated as serious. Although the issues don't affect OS X versions prior to 10.4., and no exploits have been reported, Symantec assigned its highest severity rating −− 10 out of 10 −− to the vulnerabilities in an advisory issued Tuesday afternoon to subscribers of its DeepSight Threat Management System.
Source: http://www.crn.com/sections/breakingnews/breakingnews.jhtml;jsessionid=EJZFRXQHONR5YQSNDLRSKHSCJUNN2JVN?articleId=189602 092

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for an unpatched buffer overflow vulnerability in Microsoft Hyperlink Object Library (HLINK.DLL). By persuading a user to access a specially crafted hyperlink in an email message or MS Office document, a remote attacker may be able to execute arbitrary code with the privileges of the user.

More information about this vulnerability can be found in the following:

VU#394444 − Microsoft Hyperlink Object Library stack buffer overflow: http://www.kb.cert.org/vuls/id/394444

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited web links received in email messages or embedded in MS Office documents.

US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 38566 (−−−), 445 (microsoft−ds), 6881 (bittorrent), 33947 (−−−), 25 (smtp), 32790 (−−−), 5514 (−−−), 4672 (eMule), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *June 28, Associated Press* — **High water threatens Rockville, Maryland dam.** More than 2,200 people were evacuated from their homes in an area surrounding a Maryland lake that was approaching 25 feet above its normal level early Wednesday, June 28, Montgomery County officials said. The county ordered a mandatory evacuation overnight in the neighborhoods near Lake Needwood on the north side of Rockville after engineers observed soft and weakened spots on lake's earthen dam. "These engineers and experts became increasingly concerned about the structural integrity of that dam," said Bruce Romer, chief administrative officer for Montgomery County. "As midnight approached, they began to observe actual seepage of water and leakage of water from the dam. "The dam is failing in general, so that's why we're asking people to take what ever medications they need and leave," said Montgomery County Police Lt.

Eric Burnett. Residents were asked to leave the area and stay with family, friends, or at a shelter established at Wheaton High School. A separate shelter for families with pets was set up at the Gaithersburg fairgrounds. Engineers were inspecting the dam at first daylight to determine what could be done to strengthen its walls.
Source: http://www.baltimoresun.com/news/weather/bal−montgomery0628,0,6845751.story?coll=bal−home−headlines

[Return to top]

General Sector

31. *June 28, CNN* — **Floods cause deaths, thousands of evacuations.** From upstate New York to the Virginia coast, flooding caused at least ten deaths and forced thousands of people from their homes on Wednesday, June 28. The rising Susquehanna River spilled into the streets of Binghamton, NY, covering cars, flooding homes and prompting a mandatory evacuation of as many as 15,000 residents, officials said. About 30 miles to the northeast, a rising creek washed out a section of Interstate 88 in Sidney, NY, causing wrecks that killed two truckers and closed the highway, state police said. Governor George Pataki declared states of emergency in 10 New York counties. Rivers were still rising in Virginia after four days of downpours, and highways across the region were blocked by flooding and washouts. In northeastern Pennsylvania, hundreds of people were believed trapped in the upper floors and on the roofs of their homes as National Guard troops and a Coast Guard helicopter worked to rescue them. A U.S. Coast Guard helicopter pulled several people from the roofs in Wilkes−Barre Township and Liberty, PA, early Wednesday, and the search and rescue efforts continued, according to U.S. Coast Guard Lt. Gene Maestas. Governor Edward Rendell declared a state of emergency for 46 Pennsylvania counties.
Source: http://www.cnn.com/2006/WEATHER/06/28/east.flood/index.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer